**Chapter 7:** **RANDOM and Pseudorandom Number**

**Generation and Stream Ciphers**

**TRUE OR FALSE**

T F 1. The principle requirement of random or pseudorandom number

generation is that the generated number stream be unpredictable.

T F 2. Random numbers play an important role in the use of encryption

for various network security applications.

T F 3. There are well-defined tests for determining uniform distribution

and independence to validate that a sequence of numbers is

random.

T F 4. With true random sequences each number is statistically

independent of other numbers in the sequence and therefore

unpredictable.

T F 5. The true random number generator may simply involve conversion

of an analog source to a binary output.

T F 6. Examples of a pseudorandom function are decryption keys and

nonces.

T F 7. If the PRF does not generate effectively random 128-bit output

values it may be possible for an adversary to narrow the

possibilities and successfully use a brute force attack.

T F 8. The purpose of the Maurer's universal statistical test is to

determine whether the number of ones and zeros in a sequence

are approximately the same as would be expected for a truly

random sequence.

T F 9. The seed that serves as input to the PRNG must be secure for

cryptographic applications.

T F 10. Three broad categories of cryptographic algorithms are commonly

used to create PRNGs: symmetric block ciphers, asymmetric

ciphers, and hash functions and message authentication codes.

T F 11. A widely used technique for pseudorandom number generation is

an algorithm known as the linear congruential method.

T F 12. A cryptographically secure pseudorandom bit generator is defined

as one that passes the *least significant bit test.*

T F 13. The security of Blum, Blum, Shub is based on the difficulty of

factoring *n*.

T F 14. The stream cipher is similar to the one-time pad with a difference

being that a one-time pad uses a pseudorandom number stream

and a stream cipher uses a genuine random number stream.

T F 15. The longer the keyword the more difficult the cryptanalysis.

**MULTIPLE CHOICE**

1. A secret key for symmetric encryption that is generated for use for a short period of time is called a \_\_\_\_\_\_\_\_\_ .

A. strategic key B. sequence key

C. session key D. stream key

1. A \_\_\_\_\_\_\_\_\_\_ is used to produce a pseudorandom string of bits of some fixed length.

A. PRF B. PRNG

C. OFB PRNG D. TRNG

1. A source that is effectively random is referred to as a(n) \_\_\_\_\_\_\_\_\_\_ .

A. open source B. entropy source

C. keystream D. seed

1. A \_\_\_\_\_\_\_\_\_\_ takes as input a source that is effectively random.

A. PRF B. BBS

C. PRNG D. TRNG

1. A pseudorandom number generator takes as input a fixed value called the

\_\_\_\_\_\_\_\_\_\_ and produces a sequence of output bits using a deterministic algorithm.

A. seed B. fixed skew

C. entropy source D. keystream

1. The best that can be done to determine if a PRNG generates numbers that have the characteristic of randomness is on the basis of multiple tests. These tests should seek to establish uniformity, scalability, and \_\_\_\_\_\_\_\_\_\_ .

A. consistency B. authentication

C. frequency D. sequencing

1. The \_\_\_\_\_\_\_\_\_\_ test is the most basic test of randomness and must be included in any test suite.

A. frequency B. runs

C. unpredictability D. Maurer

1. The Blum, Blum, Shub generator is referred to as a \_\_\_\_\_\_\_\_\_\_\_\_ .

A. TRNG B. OFB PRNG

C. QRN D. CSPRBG

1. Two approaches that use a block cipher to build a PNRG and have gained widespread acceptance are:

A. CTR mode and CFB mode B. CTR mode and OFB mode

C. CBC mode and CFB mode D. OFB mode and ECB mode

1. A \_\_\_\_\_\_\_\_\_\_ uses a nondeterministic source to produce randomness.

A. CSPRBG B. TRNG

C. PRNG D. BBS

1. \_\_\_\_\_\_\_\_\_\_ is an open source project for creating truly random numbers using inexpensive cameras, open source code, and inexpensive hardware.

A. LavaRnd B. Blum, Blum, Shub

C. Maurer’s statistics D. Entropy

1. Various methods of modifying a bit stream to reduce or eliminate a bias have been developed. These are referred to as \_\_\_\_\_\_\_\_\_\_\_ algorithms.

A. backward B. deskewing

C. forward D. keystream

1. The Linux operating system uses \_\_\_\_\_\_\_\_\_ entropy sources for generating random numbers.

A. four B. three

C. one D. two

1. In key distribution and reciprocal authentication schemes two communicating parties cooperate by exchanging messages to distribute keys and/or authenticate each other. In many cases \_\_\_\_\_\_\_\_\_\_\_ are used for handshaking to prevent replay attacks.

A. session keys B. nonces

C. RC4’s D. entropies

1. The distribution of bits in a random number sequence should be \_\_\_\_\_\_\_\_\_\_\_ , therefore the frequency of occurrence of ones and zeros should be approximately equal.

A. independent B. uniform

C. reversed D. streamed

**SHORT ANSWER**

1. A stream cipher is a symmetric encryption algorithm in which ciphertext output is produced bit-by-bit or byte-by-byte from a stream of plaintext input.
2. Typically the PRF takes as input a seed plus some context specific values such as a user ID or an application ID.
3. Two criteria used to validate that a sequence of numbers is random are uniform distribution and Independence .
4. The most important and widely used stream cipher is RC4 .
5. Two distinct requirements for a sequence of random numbers are unpredictability and Randomness.
6. If the algorithm is good the resulting sequences will pass many reasonable tests of randomness. These numbers are referred to as pseudorandom numbers.
7. The entropy source is drawn from the physical environment of the computer and could include things such as keystroke timing patterns, disk electrical activity, mouse movements, and instantaneous values of the system clock.
8. An algorithm that is used to produce an open-ended sequence of bits is referred to as a PRNG .
9. The purpose of the RUNS test is to determine whether the number of runs of ones and zeros of various lengths is as expected for a random sequence.
10. A stream of pseudorandom numbers should exhibit two forms of unpredictability: forward and Backward .
11. Purpose-built algorithms are designed specifically and solely for the purpose of generating pseudorandom bit streams.
12. In a stream cipher structure a key is input to a pseudorandom bit generator that produces a stream of 8-bit numbers that are apparently random. The output of the generator, called a keystream, is combined one byte at a time with the plaintext stream using the bitwise exclusive-OR operation.
13. RC4 is a stream cipher designed in 1987 by Ron Rivest for RSA Security.
14. Operating systems typically provide a built-in mechanism for generating random numbers. For example, linux uses mouse and keyboard activity, disk I/O operations, and specific interrupts.
15. A fundamental requirement of the RSA public-key encryption scheme is the ability to generate prime numbers.